Szádeczky Tamás–Szőke Gergely László*

A bizalmasság és a nyilvánosság aktuális kihívásai az információbiztonság tükrében[1]

információbiztonság – Ibtv. – adatbiztonság – adatvédelem – titokvédelem – információszabadság

Az elmúlt évtizedekben többször felmerült, hogy a különböző technológiai megoldások miként segíthetik egyes normatív, jogszabályban foglalt előírások érvényesülését. A technológiának a jog szolgálatába állítására több konkrét példát is találni, a szerzői jogi digitális jogkezelési rendszerektől kezdve egyes médiatartalmak szűrésén[2] keresztül az adatvédelmi szabályok érvényesülését segítő megoldásokig.[3]

E technológiai megoldások fontos jellemzője, hogy igyekeznek ténylegesen megakadályozni azokat a magatartásokat, amelyeket a jogi szabályozás nem tesz lehetővé. Ugyanakkor a jogszabályok sokszor magukat a technológiai megoldásokat is védik, és például azok kijátszását szankcionálják.

Jelen tanulmány e gondolati keretrendszerben igyekszik feltárni az információbiztonsági intézkedésekre vonatkozó szabályok, és az ezen intézkedésekkel támogatott titokvédelmi és nyilvános hozzáférésre vonatkozó szabályok általános összefüggéseit, így közvetve kijelölni az információbiztonságnak a jogrendszerben elfoglalt helyét is, és rámutatni olyan ellentmondásokra, amelyek ez idáig a magyar jogirodalomban nem vagy csak marginálisan jelentek meg.

Elvi kiindulópontunk az lehet, hogy az információbiztonság szabályozásának elsősorban „támogató" funkciója van, valójában a titokvédelmi és nyilvánosságot biztosító szabályrendszer tárgyaként szolgáló adatok jogszerű kezelését hivatott biztosítani, azaz egy eszközjellegű szabályozás. A kutatás eredményeként azonban egyre inkább az látszik, hogy ezen az eszközjellegen túlmutató funkciója is van:

* Dr. Szádeczky Tamás egyetemi docens, Nemzeti Közszolgálati Egyetem Államtudományi és Közigazgatási Kar Elektronikus Közszolgálati Intézet, Budapest, szadeczky.tamas@uni-nke.hu). Dr. Szőke Gergely László egyetemi adjunktus, Pécsi Tudományegyetem ÁJK Közigazgatási Jogi Tanszék Informatikai és Kommunikációs Jogi Csoport; PTE Szentágothai János Kutatóközpont Big Data kutatócsoport, Pécs, szoke.gergely@ajk.pte.hu.

1 Az Emberi Erőforrások Minisztériuma ÚNKP-17-4-III-NKE-26 kódszámú és ÚNKP-17-4-I.-PTE-348 kódszámú, az Új Nemzeti Kiválóság Programjának támogatásával, a pályázatokban vállalt együttműködés keretében készült.

2 Polyák Gábor: Technológiai determinizmus a kommunikáció szabályozásában. *Információs Társadalom,* 2011/1–4, 31–47.

3 Balogh Zsolt György–Kiss Attila–Polyák Gábor–Szádeczky Tamás–Szőke Gergely László: Technológia a jog szolgálatában? Kísérletek az adatvédelem területén. *Pro Futuro,* 2014/4, 33–45.

olyan további, a védendő adatokhoz közvetlenül nem kapcsolódó értékek és érdekek védelmét is hivatott biztosítani, mint például az informatikai erőforrások védelme, a jogosulatlan szolgáltatáshasználat megelőzése, bizonyos jogosulatlan reálcselekmények megelőzése, és – egészen tág kontextusba helyezve – a magyar kibertér védelme.

A jelen tanulmány tárgya – e komplex téma kis szeleteként – kizárólag az információbiztonság és az adatok titokvédelmi, illetve nyilvánosságát biztosító szabályrendszer kapcsolatának jogászi szempontú vizsgálata. A tanulmány ennek keretében mindenekelőtt áttekinti, hogy az információbiztonság szabályozásának melyek az alapvető céljai, mennyiben tekinthető ez állami feladatnak, és mi a hatályos szabályozás szerkezete, logikája. Ezt követően két nagy fejezetben tárgyalja az információbiztonságot mint a szabályozás eszközét, majd mint a szabályozás tárgyát.

1. Információbiztonság mint állami (?) feladat

Az információbiztonság „az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése; továbbá, egyéb tulajdonságok, mint a hitelesség, a számon kérhetőség, a letagadhatatlanság és a megbízhatóság, szintén ide tartozhatnak”.[4] A fenti fogalom középpontba állítja azt a három, elsődlegesnek tekintett területet, ami leírja az adatok és rendszerek tekintetében azt a fogalmi hármast, amire az angol nyelvű szakirodalom CIA-triádként (confidentiality, integrity and availability) hivatkozik, és ami tulajdonképpen az információbiztonság fogalmának központi eleme. Ezek az elemek – bár sokszor szervesen összekapcsolódnak – egymástól függetlenül is értelmezhetők; egyes esetekben – mint ahogy később bemutatjuk – nem is kell minden egyes területet lefedni.

A digitális adatok tekintetében szűkebb fogalmi meghatározás, hogy „az informatikai biztonság az informatikai rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelyben annak védelme az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos”.[5]

Az adatbiztonság „az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere”.[6] Más megfogalmazás szerint „az informatikai rendszerekben az adatok kezelésének megfelelő minőségét jellemző állapot. Az adatbiztonság három összetevőre: az integritásra, a titkosságra és a pontosságra bontható.”[7] Az adatbiztonság tágabb értelmezésében az adatok (digitális vagy papíralapú) jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere. Szűkebb értelmezésében pedig a technikai adatvédelem,

[4] MSZ ISO/IEC 27001:2006 3.4. p. 22.

[5] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana. *Bolyai Szemle,* 2008/4, 145.

[6] Informatikai Tárcaközi Bizottság 8. sz. ajánlása, 1994, 132.

[7] Szabó József (főszerk.): *Hadtudományi lexikon.* Magyar Hadtudományi Társaság, Budapest, 1995, 6.

tehát a személyes adat- vagy magánszféra-védelem jogi követelményeinek a műszaki-technikai megvalósítása.[8] E tanulmányban e szűkebb értelmezést követve az adatbiztonság fogalma alatt azokat az információbiztonsági intézkedéseket értjük, amelyeknek tárgya személyes adat.[9]

Ha arra a kérdésre szeretnénk választ kapni, hogy az információbiztonság biztosítása mennyiben tekinthető állami feladatnak, és ezzel összhangban milyen alanyi körre érdemes kötelezettségeket telepíteni, több stratégiai dokumentumhoz, jogszabálytervezethez és jogszabályhoz is nyúlhatunk. A Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) számú kormányhatározat előírja az elektronikus információs rendszerek biztonságának erősítését, a létfontosságú nemzeti információs infrastruktúra védelmének fokozását, továbbá a megfelelő kibervédelem kialakítását. Így ez mint állami feladat megjelenik. Tovább részletezve a Nemzeti Biztonsági Stratégiában irányelvként megfogalmazottakat, a Kormány elkészítette Magyarország Nemzeti Kiberbiztonsági Stratégiáját is.[10] A jogalkotó úgy vélte, hogy a világban a közelmúltban tapasztalt kiberháborúk indokolják, hogy ennek keretében elkészüljön egy korszerű magyar információbiztonsági törvény is, így 2013. április 25-én – a közigazgatási informatika szabályozásában hatalmas mérföldkőként – kihirdették az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényt (Ibtv.).

A törvény hatálya a cím és a 2. §-ban meghatározott személyi hatály alapján elsőre gondoltnál jelentősen szélesebb körű, mivel az kiterjed a jogszabályban meghatározott, a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozóira és az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemekre is.[11] Ezek a szervek jelentős mértékben bővíthetik (akár gazdasági társaságokkal is) a személyi hatályt, így tipikusan a közüzemi szolgáltatók, elektronikus hírközlési szolgáltatók, pénzügyi szervezetek kerülnek a kötelezetti körbe, tételes listát azonban a törvény nem tartalmaz. A törvény alapvető információbiztonsági követelményként az elektronikus információs rendszerben kezelt adatok és információk bizalmasságát, sértetlenségét és rendelkezésre állását írja elő.[12]

[8] Definíció nélkül alkalmazza a fogalmat az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) a 6. címszavában, ahol információbiztonsági jellegű kontrollokat ír le a személyes adatok védelmében.

[9] Személyes adat: az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés, míg az érintett: bármely meghatározott, személyes adat alapján azonosított vagy – közvetlenül vagy közvetve – azonosítható természetes személy (Infotv. 3. § 1–2. pont). Tartalmilag ezzel lényegében megegyező definíciót ad a hamarosan Magyarországon is közvetlenül alkalmazandó új európai adatvédelmi rendelet, a GDPR is [Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)].

[10] 1139/2013. (III. 21.) Korm. sz. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.

[11] Ibtv. 2. § (2) b)–c) pont.

[12] Ibtv. 5. § a) pont.

Az Ibtv. részletes indokolása[13] szerint *„az értelmező rendelkezések az elfogadott és általánosan alkalmazott hazai szakkifejezésekre épülnek. Ezek jelentős része a Kormány 3296/1991. (VII. 5.) határozata alapján 1991. november 27-én létrehozott Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága 12. számú ajánlásaként 1996. április 2-án elfogadott Informatikai Rendszerek Biztonsági Követelményei című dokumentumban rögzítésre került. Az itt leírt fogalmak és definíciók az Informatikai Biztonság Kézikönyve (Verlag Dashöfer, Budapest, 2000–2005), illetve a Közigazgatási Informatikai Bizottság 25. és 28. számú ajánlásaiban is megjelentek, a nemzetközi szakirodalmat, szabványokat figyelembe véve, újra feldolgozva korábbi definíciókat."* Ezzel a jogalkotó figyelembe vette a '90-es években széles szakmai körben elterjedt ajánlásokat, illetve – mivel a hivatkozott Közigazgatási Informatikai Bizottság 25. sz. ajánlása az ISO 27001 és az ISO 27002 alapján készült – nemzetközi információbiztonsági szabványok is megjelennek benne.

A törvény előírja az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása, illetve az abban kezelt adatok és információ bizalmassága, sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és kockázatokkal arányos védelmét.[14] Fontos, hogy a kockázatokkal arányos védelem és így a kockázatértékelés explicit módon bekerüljön az állami információbiztonsági követelmények közé, ugyanis sok esetben az a tapasztalat, hogy inkább ad hoc módon, a rendelkezésre álló költségvetéshez mérten történt a védelem kialakítása.

Annak érdekében, hogy az Ibtv. hatálya alá tartozó elektronikus információs rendszerek, valamint az azokban kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen, az elektronikus információs rendszereket be kell sorolni egy-egy biztonsági osztályba a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából. A biztonsági osztályba sorolás alkalmával – az érintett elektronikus információs rendszer vagy az általa kezelt adat bizalmasságának, sértetlenségének vagy rendelkezésre állásának kockázata alapján – 1-től 5-ig számozott fokozatot kell alkalmazni, a számozás emelkedésével párhuzamosan szigorodó védelmi előírásokkal együtt.[15] Nehézséget okozhat az alkalmazásnál, hogy az „egy-egy" kifejezésből az adódna, hogy a CIA-faktorok közül mindháromban egy-egy besorolást kell adni, a törvény további szakaszaiból azonban ez nem következik. Bár a biztonsági osztályba sorolás elsősorban az adatok biztonsági besorolásán múlik, a törvény nem határozza meg, hogy az adatoknak milyen minimális biztonsági szintnek kell megfelelniük. Ezzel szemben a 9. § (2) bekezdése a különböző szervezeteknek határoz meg minimális biztonsági besorolást. Ez a közszféra „energiaminimumra" való törekvése alapján részben azt eredményezte, és várhatóan továbbra is azt fogja eredményezni, hogy az adatok védelmi igényét nem fogják értékelni, csak a lenti listából fognak kiindulni. Ez a folyamat és értékelés még a mai napig nem zajlott le teljes körűen. Ráadásul a törvény 7. § (5) bekezdése alapján a szervezet vezetője

[13] Ibtv. 1. §-hoz fűzött részletes indokolás, http://www.parlament.hu/irom39/10327/10327.pdf (2018. 03. 11.).

[14] Ibtv. 5. § b) A szabályozás tárgyának meghatározása – amely tehát nemcsak a rendszerben kezelt adatok, hanem magának a rendszernek a védelmét is előírja – is azt mutatja, hogy a szabályozás célja szélesebb körű, mint pusztán kiszolgálni az adatok védelmére vonatkozó előírásokat.

[15] Ibtv. 7. § (1)–(2) bekezdés.

„kivételes esetben indoklással ellátva alacsonyabb biztonsági osztályt is megállapíthat". Az egyetlen dolog, ami érdemben meg tudja akadályozni ezt a „lefelé licitálást", a Nemzeti Elektronikus Információbiztonsági Hatóság szigorúsága, amit az Ibtv. 9. § (4) tesz lehetővé.

Az Ibtv. 11. § (1) c) pont alapján a kötelezett szervezet vezetője az elektronikus információs rendszer biztonságáért felelős személyt nevez ki, aki felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért, ami bár egy hagyományos CISO feladatköre a felsorolás[16] alapján, a neve és a feladatkörének definíciója mégis arra utal, hogy a szervezet első számú vezetőjét és a szervezet dolgozóit mentesíti információbiztonsági kötelezettségeik és felelősségeik alól.

Az Ibtv. megalkotásakor a Nemzeti Fejlesztési Minisztérium keretében létrehozta a Nemzeti Elektronikus Információbiztonsági Hatóságot és a sérülékenységvizsgálat és forenzikus logelemzés elvégzéséhez szakhatóságként a Nemzeti Biztonsági Felügyeletet is bevonja a tevékenységébe.[17] A kormányzati CERT[18] feladatait a megszűnt Puskás Tivadar Közalapítványtól a Nemzetbiztonsági Szakszolgálathoz, létfontosságú rendszerelemek tekintetében pedig a katasztrófavédelemnél működő Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központjához (LRLIBEK) helyezi át.[19]

Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelettel ez a struktúra annyiban változott, hogy a Nemzeti Elektronikus Információbiztonsági Hatóság a Belügyminisztérium alá tartozó Nemzetbiztonsági Szakszolgálathoz került, ezzel létrehozva a Nemzeti Kibervédelmi Intézetet, amelyben a fenti hatáskörök összpontosulnak.

Az Ibtv. 23. § alapján a Nemzeti Közszolgálati Egyetem dolgozta ki az elektronikus információs rendszer biztonságáért felelős személyek és érintett szervezetek munkatársainak képzését, ami azóta is minden félévben induló szakirányú továbbképzési szak, illetve közszolgálati továbbképzés formájában fut.

Összességében az utóbbi évek tendenciája határozottabb jogi szabályozást mutat, részben akár a technikai szabályok jogi normákba ültetésével. Ettől hosszú távon jelentős társadalmi hatás várható. Valószínűleg a szabványon alapuló rendszerek is szaporodni fognak, tekintettel arra, hogy ha a gazdasági társaság egyébként is betartja az informatikai biztonságra vonatkozó szabályokat, akkor marketingokokból, illetve a cég sikeresebb külföldi megjelenése érdekében valamely nemzetközi informatikai biztonsági szabvány alapján is tanúsíttatni fogja rendszerét. A szabályozás nagyobb biztonságot fog eredményezni, hosszabb távon csökkenni fog az informatikai és kommunikációs technológiák területén a nemzeti biztonsági kockázat. Mindezek mellett az Ibtv., bár jó lépés a megfelelő szintű kormányzati információbiztonsági

[16] Ibtv. 13. § (2) bekezdés.
[17] Ibtv. 18. §.
[18] Computer Emergency Response Team, az informatikai vészhelyzeteket/incidenseket kezelő szervezet.
[19] Ibtv. 19. § (6) bekezdés.

ság irányába, egyelőre túl sok felelőst nevez meg, és kibúvókat biztosít a szabályok alkalmazása alól.

Ezekből látható, hogy az utóbbi években a kormány állami feladatként (is) tekint az információbiztonság kikényszerítésére az állami és ahhoz közvetlenül kapcsolódó szektorokban. Ezt erősíti a közösségi a szabályozás is: az egységes digitális piac stratégia keretében megalkotott rendeletek és irányelvek. Ezek közül kiemelendő a NIS-irányelv,[20] amely előírja a tagországok számára az információbiztonsági stratégia megalkotását (meghatározott tartalmi elemekkel), valamint az informatikai incidensek kezelésének hatékonyabb módját, európai szinten is.

A fentiekben tehát elsősorban mint állami feladat jelent meg az információbiztonság. Ebben az esetben a kormányzat jellemzően a kezelésében lévő személyes, minősített, döntés-előkészítő vagy hasonló megítélés alá tartozó adatot, vagy pedig magát a rendszert mint futó szolgáltatások összességét, tehát az adatok védelmét ellátó rendszereket, azokat támogató rendszerelemeket és általában mint erőforrást védi.[21]

Jelenleg az üzleti szférára (leszámítva egyes különleges elemeket, mint a kritikus infrastruktúrák), illetve a magánszemélyek számítógépeire és adataira – az általános adatbiztonsági követelményeket leszámítva – nincsen részletes információbiztonsági intézkedésekre vonatkozó előírások. Aki úgy látja jónak, természetesen bevezethet bármilyen szabványalapú vagy ad hoc kontrollintézkedés-csomagot, nyitva áll az önszabályozás lehetősége. Teszik is ezt sokan, különösen azon nagyobb szervezeteknél, ahol a felső vezetés belátja ennek szükségességét, és megfelelő erőforrásokkal is rendelkezik hozzá.

Szakmai szempontból az információbiztonság tehát egy mindenki számára kívánatos, de nem kizárólagosan állami feladat. Az államnak a saját rendszerei és az állam saját, illetve az állampolgárok adatainak a kezelése tekintetében mindenképpen felmerül az állam információbiztonsági feladata is. A hatósági ellenőrzés ezen belül egy kizárólagosan állami feladat, ahol ezt az adott kormány felvállalja. Véleményünk szerint kívánatos lenne a jelenleg hatályos Ibtv. hatálya mellett (nem azonos szabályozási mélységgel és kontrollrendszerrel) a gazdasági szféra adatait és rendszereit is szabályozni, akár az adatbiztonsági intézkedésekre vonatkozó általános szabályok, akár a Ptk. szerinti üzleti titok védelmének szakmai tartalommal való kitöltése érdekében.

2. Információbiztonság mint (szabályozási) eszköz

Amint azt korábban említettük, az információbiztonság szabályozásának van egyfajta eszközjellege: kiszolgálja és segíti a jogszabályi megfelelést az adatvédelem, a titokvédelem és a közérdekű adatok nyilvánosságára vonatkozó szabályozás területén. Érdemes áttekinteni ennek jogszabályi megvalósulását.

[20] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.

[21] Erre utalhat az Ibtv. 5. § a) és b), ahol az elektronikus információs rendszerben kezelt adatok és információk és az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása, zárt, teljes körű, folytonos és kockázatokkal arányos védelme is követelményként jelenik meg.

2.1. Adatbiztonság és adatvédelem

2.1.1. Adatbiztonság mint az adatvédelmi megfelelés eszköze

A személyes adatok védelmének szabályozása során szinte első ránézésre is evidens az információbiztonság személyes adatokra vonatkoztatott követelményeinek, azaz az adatbiztonságnak a kiemelt szerepe. Az adatbiztonságra vonatkozó szabályok azt várják el az adatkezelőtől, hogy megfelelő technikai és szervezési intézkedéseket hajtson végre a vonatkozó jogszabályok érvényre juttatása, azaz a személyes adatok tényleges védelme érdekében. Az új európai adatvédelmi rendelet, a GDPR[22] is megerősíti e korábban is létező szabályrendszert.

A személyes adatok védelme szempontjából a bizalmasság, sértetlenség és rendelkezésre állás biztosítása egyaránt a jogszabályi megfelelés elengedhetetlen eszköze: a jogosulatlan hozzáférés megakadályozása, mint az adatvédelmi szabályozás központi eleme, az adatok pontosságának és naprakészségének követelménye, valamint az érintettek hozzáférési joga is csak akkor biztosítható, ha mindhárom fenti követelmény teljesül.

E megközelítés alapján tehát az adatvédelem és adatbiztonság „kéz a kézben" járnak, minél erősebbek, átfogóbbak az adatbiztonsági intézkedések, annál jobban szolgálják az adatvédelmi szabályok érvényesülését és az adott adatkezelő adatvédelmi szabályoknak való megfelelését.

2.1.2. Az információbiztonság és adatvédelem konfliktusa

Érdemes azonban egy másik, az adatkezelő szintjén is megjelenő nézőpontra rávilágítani: arra, hogy a konkrét adatbiztonsági (illetve ennél általánosabban: információbiztonsági) intézkedések és az érintettek magánszféra-védelmét biztosító adatvédelmi szabályozás könnyen konfliktusba is kerülhet egymással.[23] Ez egyszerű okra vezethető vissza: ezen intézkedések alkalmazása sokszor olyan adatkezeléssel, az érintettek magatartásának esetleges megfigyelésével, sőt akár profilozásával és viselkedéselemzésével jár együtt,[24] amelynek során két szembe nálló érdekként is lehet e területekre gondolni.

A témakör tágabb kontextusa, mint a „biztonság és magánszféra-védelem konfliktusa", már-már klasszikus kérdésnek számít, számtalan tanulmány és elemzés foglalkozik e kérdéssel világszerte, igaz, elsősorban az államok mozgásterére, az állami szabályozásra vagy az alapjogi és rendes bírósági gyakorlatra koncentrálva.[25]

[22] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet).

[23] Szádeczky Tamás: Az IT biztonság szabályozásának konfliktusa. *Infokommunikáció és Jog,* 2013/56, 149–153.

[24] Kiss Attila–Krasznay Csaba: A felhasználói viselkedéselemzés kiberbiztonsági előnyei és adatvédelmi kihívásai. *Információs Társadalom,* 2017/1, 58–60.

[25] A több évtizedre visszanyúló nemzetközi és hazai jogirodalom közül csak a legújabb fejleményekre utalva két szakfolyóirat is tekintélyes tematikus blokkot, illetve számot szentelt e kérdéskörnek (*Replika,* 2017/3, *Információs Társadalom,* 2017/1.)

Az egyensúly kényes, és a közelmúltban a szakirodalom kezdte is meghaladni a sokáig érvényesülő „trade-off" szemléletet, amely e két érdek érvényesülését alapvetően egymás kárára megvalósíthatónak tekintette. Empirikus kutatások alapján ugyanis úgy tűnik, hogy ha az emberek bizonyos szituációkban hajlamosak is önként alkut kötni a magánéletük és a biztonságuk érvényesítése között, az „azonban kijelenthető, hogy gondolkodásukban a privacy és a biztonság alapvetően két egymástól független érték, és a többségük mind a kettőt fontosnak tartja".[26] Ezen értékek – megfelelő módszertannal – jobban kiegyensúlyozhatóak lennének a bírói gyakorlatban és más döntéshozatali eljárás során is.[27]

Az egyensúlyra törekvés az adatkezelők szintjén is létfontosságú, és ez talán kevesebb figyelmet kapott ez idáig. Az államnak ugyanis viszonylag széles hatásköre van – a nemzetközi jogi és az adott állam alkotmányos keretei között – az egyik vagy másik értéknek nagyobb prioritást biztosítani, és bár a nem megfelelő megoldások különböző szankciókkal járhatnak az államok számára is (a társadalmi károkról nem is beszélve), egy adatkezelő lehetőségei korlátozottabbak. Az adatkezelőnek is lehet ugyan bizonyos mérlegelési lehetősége, de ha bármelyik irányba lényegesen „elbillen", jogsértést és annak meglehetősen szigorú szankcióit kockáztatja: ha nem elég magas az adatbiztonság szintje, akkor azért, ha viszont azt túlzó mértékű adatkezeléssel biztosítja, akkor pedig azért kell adott esetben felelnie.

Ez a dilemma a hazai adatvédelmi szabályozásban az Avtv. jogalaprendszerében lényegében kezelhetetlen volt. Az új jogalapokkal 2012-től, majd a GDPR alkalmazásától kezdve ez a helyzet változott, és az adatvédelmi jog keretein belül elviekben kezelhető e kérdés. Az adatbiztonság egyértelműen legitim adatkezelési célként jelenik meg,[28] az adatkezelésnek pedig vagy törvényi szabályozás, illetve jogszabályi kötelezettség (pl. épp egyes konkrét GDPR követelményeknek való megfelelés vagy az Ibtv. rendelkezéseinek betartása), vagy érdekmérlegelés lehet a jogalapja.[29] Utóbbi keretében lényegében szintén egy szükségességi-arányossági teszt elvégzésére van szükség, amelynek eredménye meghatározza az adatkezelés terjedelmét és feltételeit. A legitim cél és a megfelelő jogalap mellett is be kell tartani természetesen az adatvédelmi szabályozás valamennyi követelményét.

2.2. Információbiztonság a titokvédelmi szabályok szolgálatában

Érdemes megnézni, hogy az információbiztonsági szabályok miképpen szolgálják a titokvédelmi szabályok érvényesülését. A jogrendszerben számos olyan titokvédelmi szabály található, amelyek meghatározott adatok bizalmas kezelését írják elő. Ezek szabályozása eltérő jogterületekhez kapcsolódnak, és jelentős különbségek

[26] Székely Iván–Somody Bernadette–Szabó Máté Dániel: Biztonság és magánélet – I. rész. Az alkumodell megkérdőjelezése és meghaladása. *Replika,* 2017/3, 34.

[27] Székely Iván–Somody Bernadette–Szabó Máté Dániel: Biztonság és magánélet: az alku-modell megkérdőjelezése és meghaladása II. rész (Jogi és döntéstámogatási megközelítések). *Információs társadalom,* 2017/1, 15–20.

[28] Ld. kifejezetten erről a GDPR 49. preambulumbekezdését.

[29] Kiss–Krasznay: i. m., 63–65.

tapasztalhatók a védelem alapjául szolgáló indokok, a titokká minősítés, a jogsértések szankciói és a szabályrendszer részletezettsége kapcsán is. Erre tekintettel e tanulmány keretei között csak az információbiztonság és az üzleti titok, illetve a minősített adatok védelmének viszonyára térünk ki.

Az üzleti titok hatályos szabályozása kapcsán nem találunk közvetlen utalást információbiztonsági szabályok alkalmazására, de az üzleti titok fogalmának fontos eleme, hogy az „nem közismert", „nem könnyen hozzáférhető" és a „titok megőrzésével kapcsolatban a vele jogszerűen rendelkező jogosultat felróhatóság nem terheli".[30] E fogalmi elemeket a nemrég elfogadott, és 2018. június 9-ig a magyar jogba is átültetendő üzleti titok irányelv[31] is tartalmazza, azaz továbbra is feltétele lesz az üzleti titoknak a „titkosság" és az, hogy a „titokban tartása érdekében az információ feletti ellenőrzést jogszerűen gyakorló személy a körülmények figyelembevételével elvárható lépéseket megtette".[32]

Ezeknek a kritériumoknak természetesen számos módon meg lehet felelni, de az elsőre is nyilvánvalónak látszik, hogy ezen adatok védelme elsősorban megfelelő technikai szervezési intézkedésekkel biztosítható. Ezek hiánya, megléte és a védelem szintje nagy jelentőségű lehet egy olyan jogvitában, amelyben a titokban tartással kapcsolatos magatartásokat kell értékelni. Így a különböző információbiztonsági megoldások e területen olyan eszköznek tekinthetők, amelyek alkalmazása ugyan nem konkrétan előírt feltétel, de nagyban segíti azt, hogy az adott adat a jogszabályok alapján üzleti titoknak minősüljön – és természetesen fontos szerepe lehet az üzleti titok valódi titokban tartásában is.

Az üzleti szereplők adatainak rendelkezésre állása és sértetlensége emellett is számos szempontból fontos lehet, a szerződéses kötelezettségek teljesítésétől kezdve a legkülönbözőbb jogszabályi kötelezettségeknek – pl. számviteli, adózási vagy bármilyen adatszolgáltatási kötelezettségnek – való megfeleléshez és ezen megfelelés igazolásához is.

Az üzleti életben – kötelező jogszabályok hiányában – fontos szerep jut az információbiztonsági szabványoknak; az ezeknek való megfelelés kommunikálása bizalmat ébreszthet, és így versenyelőnnyel járhat a vállalkozások számára.

A minősített adatok védelme területén kifejezetten törvényi előírás alapján szükséges a megfelelő biztonsági intézkedések kialakítása. A minősített adat védelméről szóló 2009. évi CLV. törvény (Mavtv.) előírja, hogy minden olyan szervnél, ahol minősített adatot kezelnek, meg kell teremteni a minősített adat védelméhez szükséges, az adat minősítési szintjének megfelelő, a törvényben és a végrehajtására kiadott rendeletekben meghatározott személyi, fizikai és adminisztratív feltételeket. Ha a szerv a minősített adatot elektronikus információs rendszeren kezeli, az elektronikus információbiztonságról szóló törvényben és a végrehajtásukra kiadott jogszabályokban meghatározott elektronikus biztonsági feltételeknek is meg kell felelni.[33] Emellett

[30] 2013. évi V. törvény a Polgári Törvénykönyvről (Ptk.) 2:47. § (1) bekezdés.

[31] Az Európai Parlament és a Tanács (EU) 2016/943 Irányelve (2016. június 8.) a nem nyilvános know-how és üzleti információk (üzleti titkok) jogosulatlan megszerzésével, hasznosításával és felfedésével szembeni védelemről.

[32] 2016/943/EU Irányelv, 2. cikk 1. a) és c) pont.

[33] Mavtv. 10. § (4).

megjelenik, hogy „elektronikus biztonsági intézkedéseket kell tenni az elektronikus rendszeren kezelt minősített adat és az elektronikus rendszer bizalmassága, sérthetetlensége és rendelkezésre állása érdekében”.[34] Ezzel a jogalkotó utal a korábban is bemutatott CIA-triád alkalmazási szükségességére.

Ezen védelmi intézkedések egyik kiemelt részterületével, a rejtjeltevékenységgel kapcsolatos részletszabályokat a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V. 6.) Korm. rendelet határozza meg.

2.3. Információbiztonság az információszabadság szolgálatában

A közérdekű adatok megismeréséhez és terjesztéséhez való jog érvényesítése szempontjából az információbiztonsági szabályok szerepe elsőre talán csekélyebbnek tűnik, mivel a bizalmasság biztosítása háttérbe szorul. Ugyanakkor a másik két funkció, a sértetlenség és a rendelkezésre állás az információszabadság érvényesülése szempontjából is fontos. Az Infotv. jelenleg hatályos[35] 7. § (2) bekezdését ugyan az adatvédelmi követelményekre szokás érteni, de a jogszabályhely valójában azt várja el az adatkezelőtől, hogy megfelelő technikai szervezési intézkedéseket tegyen és eljárási szabályokat alakítson ki „e törvény” érvényre juttatása érdekében – márpedig az Infotv. a közérdekű adatokkal kapcsolatos szabályokat is tartalmaz, és kifejezetten utal is a rendelkezésre állásra és a pontosságra.[36] E követelmények hangsúlyosan megjelennek a közadatok újrahasznosításáról szóló szabályozásban is, ahol e kritériumok biztosítása a szerződésszerű teljesítés feltétele is egyben.[37] A közérdekű adatok fokozott védelmét számos – végül nagyrészt más jogszabályba beépített – rendelkezéssel biztosítja a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény. Az Ibtv. pedig egészen részletes információbiztonsági szabályokat állapít meg számos közfeladatot ellátó szerv részére is.

Összességében tehát az információbiztonsági szabályoknak a közérdekű adatok nyilvánosságában betöltött kiemelt szerepe is egyértelműen megállapítható.

3. Információbiztonság mint a jogi szabályozás tárgya

A tanulmány bevezetőjében már utaltunk arra, hogy bár elsőre talán az információbiztonsági intézkedések csupán más szabályok érvényesülését biztosító szabályrendszernek tűnnek, a tényleges helyzet ennél összetettebb, és a jogalkotó ezen intézkedéseket szabályozás tárgyává is teszi. Ez kettős célból is történhet: egyrészt azért, hogy ezen (eszközjellegű) intézkedéseket önmagában jogi védelem-

[34] Mavtv. 10. § (7).
[35] A cikk kéziratának lezárása 2018. április 30.
[36] Infotv. 26. § (1), 32. §.
[37] Közadat tv. 17 §.

ben részesítse, jelentősen növelve ezzel a hatékonyságukat, de sok esetben önálló, a titokvédelem és nyilvánosságszabályozás céljától részben független értékek védelme érdekében teszi.

Az információbiztonság területén – függetlenül a szabályozás céljától – két vizsgálódási aspektust azonosítottunk: az egyik ezen intézkedések nyilvánosságának vagy titkosságának biztosítása, a másik az előírt intézkedések be nem tartásának vagy kijátszásának következményei. A tanulmány témájából adódóan elsősorban az első kérdésre koncentrálunk.

3.1. Az információbiztonsági megoldások megismerhetősége

Az egyes információbiztonsági intézkedések rendkívül sokrétűek lehetnek, az informatikai arzenál és a szervezési intézkedések, a konkrét eljárásrendek vagy épp konfigurációs beállítások száma szinte végtelen. Viszonylag könnyen belátható, hogy minél inkább átláthatók ezek az intézkedések a potenciális támadók számára, annál könnyebb ezek kijátszása, megkerülése, azaz a sérülékenység egyértelműen nő.

Információbiztonsági szakmai szempontból nézve a kérdést a szervezet információbiztonsági politikája – amely egy magas szintű dokumentum – a szervezeten belül kötelezően nyilvános. Tájékoztatja az érdekelt feleket az információbiztonsági célokról és a szervezet felső vezetőinek információbiztonsági elkötelezettségéről.[38] Emellett ez a dokumentum lehet teljesen nyilvános, mintegy PR-eszköz is, ezért célszerű úgy megírni, hogy az ne jelentsen információbiztonsági kockázatot. Az intézkedések részletkérdéseinél azonban nem ez a helyzet, annak megismerhetősége ugyanis jelentős biztonsági kockázatot jelent. A részletes információbiztonsági szabályok, technikai beállítások, paraméterek alapvetően bizalmasan kezelendőek. Erre utal az ISO 27001 7.5.3. „A dokumentált információk felügyelete" pontja, miszerint megfelelően védve kell legyenek a bizalmasság elvesztésétől, helytelen használattól vagy a sértetlenség elvesztésétől,[39] valamint az A.18.1.4 „A feljegyzések védelme" pontja is, miszerint a „feljegyzéseket védeni kell […] a jogosulatlan hozzáféréstől vagy a jogosulatlan kiadástól, összhangban a jogi, szabályozói, szerződéses és üzleti követelményekkel".[40] Az, hogy melyik dokumentumot milyen védelemben kell részesíteni, kockázatelemzés alapján állapítható meg. Fontos, hogy ezeket a dokumentumokat jellemzően még a szervezeten belül sem hozzák nyilvánosságra, azokhoz csak egy jól meghatározott kör férhet hozzá.

E szabványokkal és kialakult joggyakorlatokkal szemben az információbiztonsági intézkedések nyilvánossága vagy titkossága a hazai jogszabályi környezet alapján korántsem egyértelmű.

[38] MSZ ISO/IEC 27001:2014 5.2.
[39] MSZ ISO/IEC 27001:2014 7.5.3.
[40] MSZ ISO/IEC 27001:2014 A.18.1.4.

3.1.1. Az információbiztonsági intézkedések mint közérdekű adatok

Amint azt a korábbiakban bemutattuk, az információbiztonsági szabályozás kiemelt alanyai egyes közfeladatot ellátó szervek. Az általuk kezelt adatok azonban – amellett, hogy a nemzeti adatvagyon részeként védelmi típusú szabályok is vonatkoznak rájuk – részben olyan közérdekű adatok, amelyek nyilvánosságát alapvető jog garantálja. A közérdekű adat fogalma meglehetősen tágan magában foglalja *„az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ[t] vagy ismeret[et], függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől”.*

Az adott szerv által alkalmazott információbiztonsági intézkedések – ideértve ennek részletkérdéseit is – álláspontunk szerint alapvetően e fogalom hatálya alá tartoznak. Az információszabadság célja felől közelítve is könnyen lehet úgy érvelni, hogy az adott szerv működésének vagy a közpénzfelhasználás célszerű elköltésének ellenőrzése szempontjából is fontos eleme a társadalmi kontrollnak, hogy az adott szerv megfelelően biztosítja-e a kezelésében lévő adatok tényleges védelmét, és az intézkedésekkel arányos közpénzt költ-e el erre. Ezek alapján elsőre úgy tűnik, mintha az információbiztonsági intézkedések – mint közérdekű adatok – széles körben megismerhetőek lennének.

A közérdekű adatok megismeréséhez való jog azonban nem korlátlan. Maga az Infotv. is felsorolja, hogy mely érdekek mentén korlátozhatja – az adatfajták meghatározásával – azt más törvény, és két konkrét korlátot – a minősített adatokra és a döntés megalapozását szolgáló adatokra vonatkozóan – maga is említ, illetve szabályoz. Bármilyen korlátozás azonban szükségszerűen csak törvényben írható elő, ami nem elsősorban az Infotv. 27. §-ból, hanem sokkal inkább az Alaptörvénynek az alapjog-korlátozásról szóló szabályaiból következik.

Az információbiztonságra tekintettel azonban nem találunk ilyen nyilvánosságkorlátozó szabályt,[41] ami mindenképpen különös: az Ibtv. elég részletes szabályokat tartalmaz az információbiztonságra nézve, kitérve a „szervezeteknek az elektronikus információs rendszereik védelmét biztosító kötelezettségeire” is, amely azonban a bizalmasságról vagy nyilvánosságról egyáltalán nem szól.[42] Érdekes, hogy a törvény foglalkozik viszont a felügyeleti hatóság adatkezeléseivel, deklarálva, hogy a

[41] Érdekes, hogy egy szűk területen a közadat-újrahasznosítás kapcsán ez mégiscsak felmerül. E szabályozás tárgya szintén közérdekű és közérdekből nyilvános adatok, és az újrahasznosításuk során az információbiztonság korlátként jelenik meg, igaz, csak a közérdekű adatokkal kapcsolatos metaadatok megismerésének korlátjaként, ld. a közadatok újrahasznosításáról szóló 2012. évi LXIII. törvény 16. §-át.

[42] Ibtv. 11–13. §§. Érdekes, hogy a törvény kitér viszont a felügyeleti hatóság adatkezeléseire, deklarálva, hogy a „hatóság eljárása során keletkezett adatok nem nyilvánosak” [Ibtv. 22. § (3) bek.]. Kérdéses, hogy ez az egymondatos deklaráció miként felel meg az alapjogkorlátozás általános szabályainak. Az Ibtv. olvasása kapcsán az olvasóban az az érzés alakulhat ki, hogy annak szövegezése során inkább az információbiztonsági intézkedések (legalábbis annak részletkérdései) bizalmasságából indult ki a jogalkotó, és egyáltalán nem foglalkozik a közérdekű adatokkal való viszony bármilyen rendezésével.

„hatóság eljárása során keletkezett adatok nem nyilvánosak" [Ibtv. 22. § (3)]. Kérdéses, hogy ez az egymondatos deklaráció miként felel meg az alapjog-korlátozás általános szabályainak. Az indokolás[43] mindenesetre tanulságos: *„A Ket. lehetővé teszi, hogy a törvény az eljárás során keletkezett iratok nyilvánosságát korlátozza. A biztonsági események, sérülékenységek és a nyilvánosság nagymértékben sebezhetővé tenné a magyar kiberteret. Ezeket az információkat fel lehetne használni súlyos és veszélyes támadások megindítására, a biztonsági rések rosszindulatú kiaknázására. Ennek megakadályozását szolgálja az Ibtv. 22. §-ának új (3) bekezdése."* Ebből egyértelműen látszik, hogy megjelent a korlátozás gondolata, de egyrészt a Ket.-re hivatkozva, holott itt alapjogi korlátozásról is szó van, másrészt e korlátot csak a felügyeleti hatóságnál vezeti be a jogalkotó, annál a – szintén közfeladatot ellátó, az Infotv. szerint közérdekű adatokat kezelő – szervnél, amelynél az adott információbiztonsági rendszer működik, és a potenciálisan veszélyt jelentő adat keletkezik, nem.

Ugyancsak találunk bizalmasságra és szűkebb körű hozzáférhetőségre utaló szabályokat az Ibtv. egyik végrehajtási rendeletében,[44] amely részletezi a szerv által megteendő intézkedéseket. Az érintett szervezet gondoskodik arról, hogy az informatikai biztonsági szabályzat jogosulatlanok számára ne legyen megismerhető, módosítható vagy hogy az információs rendszerre vonatkozó – különösen az adminisztrátori és fejlesztői – dokumentáció jogosulatlanok számára ne legyen megismerhető, módosítható, illetve gondoskodik a dokumentációknak az érintett szervezet által meghatározott szerepköröket betöltő személyek által vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismerésről.[45] E szabályok azonban nem mondanak semmit a nyilvánosság vagy megismerhetőség tartalmi kérdéseiről (és ha mondanának, akkor sem a megfelelő jogforrási szinten tennék azt), csupán előírják, hogy miként kell biztosítani a hozzáféréssel kapcsolatos szabályokat.

Az Ibtv. és e végrehajtási rendelet olvasása kapcsán összességében az olvasóban az az érzés alakulhat ki, hogy annak szövegezése során inkább az információbiztonsági intézkedések (legalábbis a részletkérdések) bizalmasságából indult ki a jogalkotó, és egyáltalán nem foglalkozik a közérdekű adatokhoz való viszony törvényi szintű rendezésével.

3.1.2. Az információbiztonsági intézkedések mint döntés megalapozását szolgáló adatok

Külön szabályozás hiányában felmerülhet, hogy az információszabadsággal kapcsolatos információk bizalmassága az Infotörvénynek a döntés megalapozását szol-

[43] A rendelkezés ebben a formában az e-kártya megvalósításához szükséges egyes törvények, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény módosításáról szóló 2015. évi CXXX. törvény 8. § (33) bekezdése iktatta az Ibtv.-ben. Az idézett indokolás a módosító törvény indokolása.

[44] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

[45] Ld. 41/2015. (VII. 15.) BM rendelet 4. sz. melléklet 3.1.1.1.1.3., 3.1.3.4.1.3. és 3.1.3.4.1.4. pontjait.

gáló adatokra vonatkozó szabályozása alapján biztosítható. Az Infotv. 27. § (5) bekezdése alapján a *„közfeladatot ellátó szerv feladat- és hatáskörébe tartozó döntés meghozatalára irányuló eljárás során készített vagy rögzített, a döntés megalapozását szolgáló adat a keletkezésétől számított tíz évig nem nyilvános”*.[46] E szabály felhívásához mindenekelőtt szükséges valamilyen döntési folyamat. Az információbiztonsági dokumentumok (pl. szabályzatok, mellékletek) előkészítése során ilyen döntési folyamat vélhetően fenn is áll, ám a különböző, napi szintű, dokumentumban nem foglalt intézkedések, beállítások stb. kapcsán a (formalizált) döntési folyamat kérdéses lehet.

A döntés meghozatala után az adat két esetben lehet továbbra is titkos. Egyrészt akkor, ha az adat további jövőbeli döntés megalapozását is szolgálja.[47] E – sokat bírált kitétel – szinte automatikusan is fennállhatna, mivel bármilyen adat szolgálhat valamilyen jövőbeli döntés alapjául, ez a széles értelmezés azonban az egész információszabadság értelmét kérdőjelezné meg. A NAIH értelmezése szerint is szűken kell értelmezni a további döntés megalapozásával kapcsolatos kitételt: „ahhoz, hogy e korlátozás megfeleljen az alkotmányos követelményeknek a döntés megalapozását szolgáló adat és a jövőbeli döntés közötti kapcsolatnak konkrétnak és közvetlennek kell lennie”.[48] „Egy bizonytalan döntéssel való absztrakt viszony ugyanakkor nem szolgálhat az információszabadság korlátozásának indokaként.”[49]

A másik eset, amikor a döntés meghozatalát követően is titokban tartható valamilyen közérdekű adat, ha annak *„megismerése a közfeladatot ellátó szerv törvényes működési rendjét vagy feladat- és hatáskörének illetéktelen külső befolyástól mentes ellátását […] veszélyeztetné”*.[50] Ennek fennállását – ahogy általában a döntés megalapozását szolgáló adat megismerhetőségét – a szerv vezetőjének kell mérlegelnie, de álláspontunk szerint az információbiztonsági intézkedések részletkérdései könnyedén e kategóriába eshetnek. Az adat keletkezésétől számított tíz év elteltével azonban ezek az adatok is nyilvánossá válhatnak.

Összességében azonban azt gondoljuk, hogy a döntés megalapozását szolgáló adatokra vonatkozó szabályozást nem szerencsés általánosságban „ráhúzni” az információbiztonsági követelményekre, hanem indokolt lenne erre tekintettel önálló kivételszabály megfogalmazása. A kivétel alapja ugyancsak az lehetne, hogy biztosítsa a közfeladatot ellátó szerv törvényes működési rendjének vagy feladat- és hatáskörének illetéktelen külső befolyástól mentes ellátását.

3.1.3. Az információbiztonsági intézkedések megismerhetősége az adatvédelmi jog alapján

Egy további terület, ahol az információbiztonsági intézkedések megismerhetősége felmerül, az adatvédelmi jogban keresendő. Ezen belül is két esetet érdemes

[46] A szerv vezetője a megismerést engedélyezheti.

[47] Infotv. 26. § (6) bekezdés.

[48] Révész Balázs–Buzás Péter: A döntés megalapozását szolgáló adatok jogi helyzete. *Pázmány Law Working Papers,* 2017/21, http://plwp.eu/files/2017-21-Revesz_Buzas.pdf (2018. 04. 14.), 17–18.

[49] A NAIH álláspontját (beszámolóját) idézi Révész–Buzás: i. m., 18.

[50] Infotv. 27. § (6) bekezdés.

megkülönböztetni: a) amikor a tájékoztatási kötelezettség azért merül fel, mert az információbiztonsági intézkedés személyes adatok kezelésével jár; b) az adott intézkedés nem jár ugyan adatkezeléssel, de olyan adatbiztonsági intézkedés, amelyről az adott intézkedéssel védett adatok érintettjeit tájékoztatni kell. Előzetesen is meg kell említeni, hogy egyik esetben sem jelenti a tájékoztatási kötelezettség teljesítése az intézkedések nyilvánosságra hozatalát, de a kellően széles körű, például az adott adatkezelő munkavállalói körében történő megismerhetőség a titokban tartást meglehetősen megnehezíti, különösen, ha a potenciális fenyegetést épp ezen alanyi körből lehet várni.

Ad a) Amint azt korábban kifejtettük, az információbiztonsági intézkedések sokszor adatkezeléssel járnak együtt, ebben az esetben pedig ennek részleteiről az érintetteket előzetesen, illetve kérelemre az adatkezelés alatt is megfelelően tájékoztatni kell. Ez kiterjed – többek között – az adatkezelés céljára, az adatkezelés jogalapjára, az érdekmérlegelésen alapuló adatkezelés esetén az érdekmérlegelés eredményére és a kezelt adatok körére is, sőt amennyiben az érintettre jelentős hatással járó, teljesen automatizált, sokszor profilozáson alapuló döntéshozatalról[51] van szó, akkor ennek tényére, az alkalmazott logikára és az érintettre nézve várható következményekre is.[52] Bár számos, az információbiztonság szempontjából is releváns érdek védelme miatt[53] maga a GDPR is lehetővé teszi valamennyi érintetti jog, így a tájékoztatáshoz való jog korlátozását, ehhez kifejezett uniós vagy tagállami jogszabály szükséges, és bár sok esetben a magyar jog is ismer ilyen korlátozásokat (például nemzetbiztonsági vagy bűnüldözési célból), általánosságban véve az információbiztonságra vonatkozóan nincs ilyen szabály.

Összességében az állapítható meg, hogy a tájékoztatási kötelezettség az adatvédelmi jog olyan alapvető jogintézménye, amely ugyan az információbiztonsági intézkedések hatékonyságát leronthatja,[54] de – a törvényben kifejezetten nevesített szabályokat kivéve – az adatkezelőnek nincs jogszerű lehetősége a tájékoztatásra vonatkozó szabályoktól eltérni.

Ad b) Ugyancsak a tájékoztatási joghoz kapcsolódik, hogy vajon az érintetti tájékoztatásnak bármely adatkezelés során ki kell-e terjednie a személyes adatait védő adatbiztonsági intézkedésekre, és ha igen, milyen mélységben. Elsőre logikus az a gondolat, hogy az érintettnek joga van tudni, hogy milyen adatbiztonsági intézkedéseket alkalmaz az adatkezelő a személyes adatai védelme érdekében, és például a hozzájáruláson alapuló adatkezelés esetén akár a hozzájárulás megadásának vagy meg nem adásának kritériuma is lehet, hogy mennyire látja az érintett biztosítottnak a személyes adatai bizalmasságát, sértetlenségét, rendelkezésre állását.

A tételesjogi szabályozás, a GDPR nem írja elő kifejezetten az adatbiztonságról szóló tájékoztatást, az erről szóló jogszabályhely ráadásul nem is példálózó, hanem

[51] Azaz megfelel a GDPR 22. cikkében szabályozott automatizált döntéshozatal feltételeinek.

[52] GDPR 13., 14., 15 cikk.

[53] Többek között nemzetbiztonsági, honvédelmi, közbiztonsági érdekből, bűncselekmények megelőzése, felderítése céljából, de akár egészen általánosan mások jogainak vagy szabadságának védelme érdekében.

[54] Ez az összefüggés ennél tágabb kontextusban is megjelenik: széles körű egyetértés van abban, hogy pl. a titkos megfigyelés növeli a megfigyeléssel elérni kívánt cél (pl. bűnmegelőzés) elérésének esélyét, de ezzel együtt abban is, hogy jogállami keretek között ez csak jogszabályban rendezett módon történhet.

tételes felsorolást ad a tájékoztatás tartalmáról. A jelenleg hatályos Infotv., valamint az Infotv. jelenleg elérhető tervezete[55] alapján bűnüldözési célból a jövőben is az adatkezelőre potenciálisan tágabb, kevésbé egzakt előzetes tájékoztatási kötelezettség vonatkozik, amely – egy példálózó felsoroláson túl – kiterjed a személyes adatok kezelésével kapcsolatos „minden tényre",[56] illetve az „adatkezelés körülményeivel összefüggő minden további érdemi" tényre.[57]

Az Infotv. 20. § (2) bekezdését a NAIH a tájékoztatási kötelezettségével kapcsolatos ajánlásában[58] úgy értelmezte, hogy *„elvárható, hogy az adatkezelők röviden és közérthetően ismertessék, milyen adatbiztonsági intézkedésekkel gondoskodnak a személyes adatok védelméről".* Az e tanulmányban tárgyalt ellentmondásra azonban a NAIH is felhívja a figyelmet: *„természetesen nem szükséges részletes felvilágosítást nyújtani az egyes adatbiztonsági intézkedésekről, hiszen ezzel veszélyeztethetik azok hatékonyságát, azonban törekedniük kell arra, hogy az érintettek megismerhessék […] a főbb intézkedéseket és azok lényegét".* Önmagában is kérdéses, hogy a GDPR zárt felsorolást tartalmazó szabályainak alkalmazásával ez az értelmezés mennyiben tartható fenn, de az jól látható, hogy a részletes adatbiztonsági intézkedések megismerésével kapcsolatban a hatóság is egyértelműen egy mérsékelt, az intézkedések hatékonyságát nem veszélyeztető álláspontot képvisel.

3.1.4. Az információbiztonsági intézkedések mint titkok

A fentieken túl a magyar jogrendszerben is számos olyan – általános vagy konkrét – jogszabályi rendelkezés található, amelyek az információbiztonsági intézkedések vagy azok egy része bizalmasságát biztosíthatja.

Az üzleti szférában nincs akadálya annak, hogy az információbiztonsági intézkedések maguk is üzleti titoknak minősüljenek, amennyiben megfelelnek az erre vonatkozó szabályozás feltételeinek. Marketingcélból az érintett vállalkozások adott esetben ugyan szívesen nyilvánosságra hozzák az alapvető információbiztonsági intézkedéseiket, ideértve különösen valamely szabványnak való megfelelést, ugyanakkor a részletek még szabványmegfelelés esetén sem nyilvánosak, azt csak a tanúsító szervezet ismerheti meg (megfelelő titoktartási és egyéb garanciális feltételek mellett), de a széles nyilvánosság nem. Fontos megemlíteni, hogy az üzleti titok fő szabályként az információszabadságot is korlátozza, igaz, közpénzfelhasználás esetén a törvény kivételt tesz, de még ebben is figyelembe kell venni, hogy – kissé ellentmondásos törvényi megfogalmazással – a nyilvánosságra hozatal *„nem eredményezheti az olyan adatokhoz – így különösen a védett ismerethez – való hozzáférést, amelyek megismerése az üzleti tevékenység végzése szempontjából aránytalan sérelmet okozna, feltéve, hogy ez nem akadályozza meg a közérdekből nyilvános adat megismerésének lehetőségét".*

[55] Infotv. 2017. augusztus 29-én, társadalmi egyeztetésre nyilvánosságra hozott verziója (Infotv. módosítástervezet). Összehasonlító szövege elérhető: https://twobirdsideas.hu/2017/09/04/az-infotv-modositasa-osszehasonlitottuk-az-im-tervezetet-a-hatalyos-torvenyszoveggel/ (2018. 04. 26.).

[56] Infotv. 20. § (2) bekezdés.

[57] Infotv. módosítástervezet 9. §-ával módosítani tervezett 16. § (2) bekezdés e) pont.

[58] A Nemzeti Adatvédelmi és Információszabadság Hatóság ajánlása az előzetes tájékoztatás adatvédelmi követelményeiről, 2015. szeptember 29., 12.

A minősített adatok kezelése tekintetében az intézkedések maguk is minősített adatok lehetnek, az általános szabályok szerint, ha azok megfelelnek a minősítés követelményeinek.[59] A törvény külön nevesíti a minősített adat kezelésére használt épület, építmény vagy annak valamely műszaki vagy technikai adata védelmét (minősíthető voltát), valamint a szokásos érvényességi időkkel szemben alkalmanként legfeljebb 10 évre, az épület, építmény használatának idejére teszi azt lehetővé.[60] Az információbiztonsági kontrollok konkrét technológiája és biztonsági követelményei a minősített adatok védelme esetén szigorú állami felügyelet mellett érvényesülnek; e feladatot a Nemzeti Biztonsági Felügyelet látja el.[61]

E területeken jól látható az egyértelmű és kölcsönös támogatás: míg az információbiztonsági szabályok (egyik) célja a titokvédelmi szabályok garantálása, addig a titokvédelmi szabályozás alkalmas arra, hogy biztosítsa az információbiztonsági intézkedések titkosságát, és így növelje hatékonyságukat.

3.2. Az információbiztonsági szabályok megsértésének következményei

Mivel nem szorosan kapcsolódik e tanulmány témájához, csak röviden teszünk említést arról, hogy a jogalkotó az információbiztonsági intézkedéseket mint szabályozási tárgyat számos más aspektusból is szabályozza, sőt az intézkedések titkosságának/nyilvánosságának kérdése tulajdonképpen marginális – mint láttuk, éppen ez okoz jogbizonytalanságot.

A jogalkotó az információbiztonsági szabályozás kapcsán él azzal a lehetőséggel, hogy az ezzel kapcsolatos szabályok megsértését a különböző jogterületeken belül szankcionálja. Csak néhány példát említve: az Ibtv. és végrehajtási rendeletei széles körű felügyeleti rendszert dolgoztak ki, és rendeltek hozzá felügyelőhatóságot, az adatbiztonsági követelmények megsértése az általános – a GDPR alkalmazásától kezdve igen szigorú – adatvédelmi felügyeleti rendszer részeként szankcionálható, de a nemzeti adatvagyon körébe tartozó állami nyilvántartásban kezelt adatok adatkezelő részére történő hozzáférhetetlenné tétele – más (jellemzően súlyosabb) bűncselekmény hiányában is büntetendő.[62]

4. Következtetések

Összefoglalva és kiegészítve e tanulmány eredményeit, mindenekelőtt megállapíthatjuk, hogy az információbiztonság és a titokvédelem, illetve egyes adatok nyilvánosságot vagy megismerhetőségét előíró szabályrendszer viszonya igen összetett. Egymásra ható, néha egymást támogató, néha viszont kifejezetten konfliktusba kerülő szabályrendszerekről van szó.

[59] Mavtv. 5. § (1)–(4) bekezdés.
[60] Mavtv. 5. § (11) bekezdés.
[61] 161/2010. (V. 6.) Korm. rendelet.
[62] A Büntető Törvénykönyvről szóló 2012. évi C. törvény 267. §.

Mindenekelőtt az látható, hogy az információbiztonság szabályozása – mind hatályát, mind részletezettségét tekintve – még mindig töredezett. A közszféra szereplőire részletesebb, az üzleti szférára és a magánszemélyekre jóval kevésbé egzakt, és alapvetően csak a személyes adatok védelmére vonatkozó szabályok találhatók.

Az is látható, hogy az információbiztonság szabályozásának jelentős, de korántsem kizárólagos eszközjellege, „kiszolgáló funkciója" van. Ennek keretében a titokvédelmi szabályozással gyakran egymást erősítve érvényesülnek: az információbiztonsági szabályok segítik az adatvédelmi, titokvédelmi szabályok vagy éppen a közérdekű adatok rendelkezésre állásának biztosítását, míg a titokvédelmi szabályok maguk is védik az információbiztonsági intézkedésekre vonatkozó adatokat.

Ennél azonban jóval érdekesebb két kifejezetten konfliktusos terület. Az első az adatbiztonsági és adatvédelmi szabályok összeütközése, amely abból ered, hogy az adatbiztonsági követelmények érvényesítése gyakran jelentős személyesadat-kezeléssel jár együtt. Ez azonban, amint arra rámutattunk, alapvetően feloldható az adatkezelő szintjén is a meglévő adatvédelmi szabályozás megfelelő értelmezésével.

Ezzel szemben a közérdekű adatok nyilvánosságára vonatkozó szabályrendszer és a közfeladatot ellátó szervek információbiztonsági intézkedéseinek titokban tartásához fűződő érdek közötti konfliktus jelenleg a szabályozás szintjén feloldatlan. Mivel a közérdekű adatok megismerése és terjesztése olyan alkotmányos alapjog, amelynek korlátozása csak az erre vonatkozó szabályok szerint, törvényben lehetséges, az adatkezelők nincsenek abban a helyzetben, hogy ezt az ellentmondást maguk feloldják. E kérdés megoldása tehát mindenképpen jogalkotói tevékenységet, törvényi szintű rendezést igényelne. A helyzet álláspontunk szerint elsősorban az Infotv. 27. §-ának az információbiztonságra utaló kiegészítésével, valamint az Ibtv. – az alapjog-korlátozás tesztjének elvégzésével kimunkált – az információbiztonsági intézkedések egyes szintjeinek bizalmasságát expressis verbis kimondó módosításával lenne feloldható.

Abstract

The paper analyses the issues of confidentiality and publicity, arising from current information security legislation in Hungary. First of all the information security as a state task is analyzed. In Hungary, the information security controls of state and local government entities are regulated. Afterward, on the one hand, the information security as a tool for data protection regulation, state secrets and freedom of information were discussed. On the other hand, information security can be an object of the law, when the protection of security controls is required. One of the main findings of the research was that the information security controls applied at state entities are generally public data (according to freedom of information regulation). Thus it might not stay confidential. We formed proposals to solve this issue.